Ejercicio 2 (Portafolio): Análisis Ético de un Caso - "La prueba sorpresa"

Objetivo: Analizar éticamente una situación en el hacking ético, identificando las acciones correctas según principios profesionales, éticos y legales, y comprendiendo las implicaciones de un fragmento de código.

Caso práctico: "La prueba sorpresa"

Un pentester junior es contratado para una auditoría de seguridad en una empresa financiera. Encuentra un archivo usuarios.db con datos sensibles accesible sin contraseña a través de una conexión interna mal configurada. Emocionado, descarga el archivo completo sin avisar y usa un script de Python para ver los datos confidenciales. Luego, pone estos datos en su portafolio personal como "prueba de habilidad", sin decir el nombre de la empresa, pero sin esconder del todo la información de los usuarios.

Preguntas de análisis ético y técnico:

1. ¿Qué principios del hacking ético han sido vulnerados? (Menciona al menos dos y explica cómo se violan)

Se vulneraron principios fundamentales:

- **Consentimiento Informado y Alcance:** El pentester debe tener permiso claro y saber hasta dónde puede llegar en sus pruebas. Aquí, descargó la base de datos y usó un script sin avisar ni tener autorización para esa acción. Actuó fuera de lo acordado con la empresa.
- **Confidencialidad:** Es la obligación de proteger la información que se encuentra. Al descargar y mostrar datos reales en su portafolio sin esconderlos bien, el pentester no protegió la privacidad de los usuarios y puso en riesgo la reputación de la empresa.

2. ¿Es válida la justificación de "fue para demostrar mis habilidades"? ¿Por qué sí o por qué no?

No, no es válida. El objetivo del hacking ético es mejorar la seguridad de la empresa, no el beneficio personal del pentester. Mostrar datos privados, incluso si no se nombra a la empresa, demuestra falta de profesionalismo y rompe la confianza. Aprender o mostrar habilidades nunca justifica romper acuerdos de confidencialidad o exponer datos sensibles. Las habilidades deben demostrarse de forma segura y sin comprometer a nadie.

3. Desde una perspectiva técnica, ¿cuál es el problema con el código presentado? (Analiza el uso, salida y exposición de datos confidenciales)

El problema con el código es que:

- **Extrae Demasiada Información:** El script saca todos los datos de la tabla de usuarios sin ningún filtro. Esto significa que se descarga una gran cantidad de información privada.
- **Muestra Datos Sensibles Directamente:** Al imprimir los datos en la pantalla, el script expone información como contraseñas o correos electrónicos en texto claro. Esto es muy inseguro, ya que cualquiera con acceso a la consola podría ver esos datos.
- **No Oculta la Información:** El script no hace nada para esconder o hacer que los datos sean irreconocibles antes de mostrarlos, lo que va en contra de la privacidad.
- **No Registra lo que Hace:** No hay un registro de cuándo se hizo la acción o desde dónde, lo que dificulta saber quién hizo qué.

4. ¿Qué medidas debió tomar el pentester una vez descubierta la base de datos sin protección? (Describe los pasos adecuados desde el punto de vista ético y profesional)

Al encontrar la base de datos desprotegida, el pentester debió:

- **Detener la Recolección de Datos:** Parar inmediatamente cualquier descarga o consulta masiva de datos.
- **Documentar la Falla:** Anotar la vulnerabilidad en un informe interno, sin incluir datos reales sensibles.
- **Avisar al Cliente Inmediatamente:** Informar de urgencia al encargado de seguridad de la empresa sobre el problema crítico.
- **Pedir Permiso para más Pruebas:** Si necesitaba más datos para demostrar la falla, debió pedir autorización explícita al cliente, especificando qué datos y cómo los manejaría.
- **Acordar un Manejo Seguro de Datos:** Si se requerían datos reales (aunque preferiblemente anonimizados), debió acordar cómo transferirlos y guardarlos de forma segura, usando canales cifrados.
- **Anonimizar Datos:** Si usaba datos para demostraciones, debieron ser completamente anónimos o modificados para que no se pudiera identificar a nadie.

5. ¿Qué implicancias legales podría enfrentar el pentester o la empresa si esta información se filtra o es identificable?

Las consecuencias legales serían graves:

- **Para el Pentester:**
    - Podría ser acusado penalmente o demandado civilmente por acceder sin permiso y divulgar información confidencial. Esto podría llevar a multas o incluso cárcel.
    - Incumpliría su contrato, lo que podría resultar en demandas por parte de la empresa.
    - Podría dañar su reputación, dificultando encontrar trabajo.
- **Para la Empresa:**
    - **Multas y Sanciones:** Podría enfrentar multas muy grandes y sanciones regulatorias por no proteger los datos personales.
    - **Demandas:** Los afectados por la filtración de datos podrían demandar a la empresa por la violación de su privacidad.
    - **Daño a la Reputación:** La imagen de la empresa se vería gravemente afectada, perdiendo la confianza de clientes y socios.

Recomendaciones éticas generales para Pentesters Junior:

Para evitar estos problemas, los pentesters junior deben:

- **Trabajar con un Contrato Claro:** Siempre tener un acuerdo firmado que defina el alcance de las pruebas y un acuerdo de confidencialidad.
- **Acceder solo a lo Necesario:** Tomar solo la información indispensable para probar una vulnerabilidad, sin descargar grandes cantidades de datos.
- **Usar Entornos Seguros y Datos Ficticios:** Realizar pruebas en ambientes aislados y usar datos falsos o anónimos para demostraciones. Si se usan datos sensibles, siempre deben manejarse con cifrado y en entornos seguros.
- **Documentar y Ser Transparente:** Registrar cada paso y ser honesto con el cliente sobre cualquier hallazgo.
- **Respetar la Ética Profesional:** Poner siempre la seguridad y la confianza del cliente por encima de cualquier beneficio personal o de mostrar habilidades.